Today
- Arthur Merlin Proof Systems
- GI - NP-complete?
- Public coins vs Private Coins

CSS.203.1
Computational Complexity
- Lecture #25
Instructor: (17 May 21)
Prahladh Harsha

Public Coins Interactive Proofs

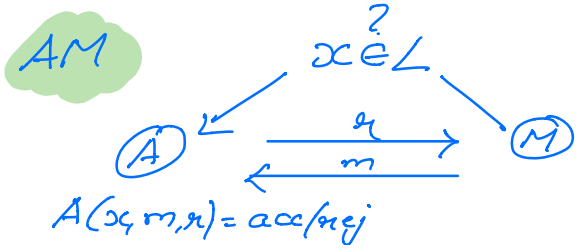
Arthur-Merlin Proofs

$AM[k(n)] = \{L \mid L$ has a public coins IP protocol w/ at most $k(n)$ rounds$\}$

$MA[k(n)]$ - Merlin (ie, prover) starts the protocol.

$AM = AM[2]$; $MA = MA[2]$

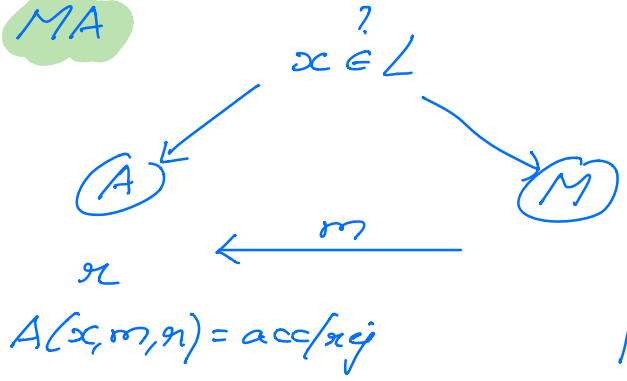
AM, MA - public coins interactive proofs w/ 2 round
(difference - who speaks first).



Comp: $x \in L \Rightarrow \Pr_r[\exists m, A(x,r,m) = acc] \geq 2/3$

Sound: $x \in L \Rightarrow \Pr_r[\exists m, A(x,r,m) = acc] \leq 1/3$.

MA



Comp: $x \in L \Rightarrow$

$\exists m, \Pr_r[A(x,m,r)=acc] \geq 2/3$

Sound: $x \notin L$

$\forall m, \Pr_r[A(x,m,r)=acc] \leq 1/3$

MA - exactly like NP, except that the det verifier is replaced by a randomized verifier.

Recall $BPP \subseteq \Sigma_2^P \cap \Pi_2^P$

R quantifier → $\exists\forall$, $\forall\exists$

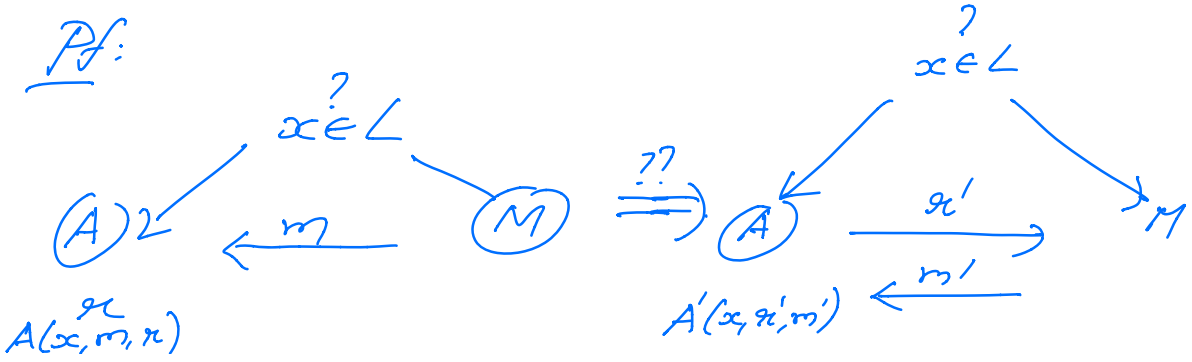
$MA \subseteq \exists\exists\forall = \Sigma_2^P$

$AM \subseteq \forall\exists\exists \subseteq \Pi_2^P$

MA vs AM.

Proposition: $MA \subseteq AM$

Pf:

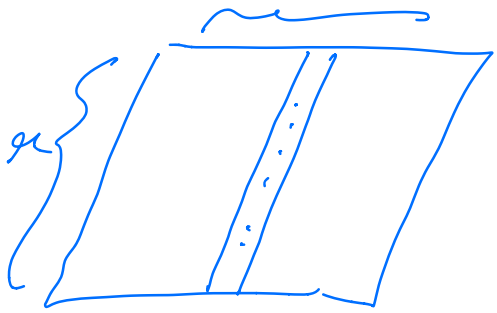


Comp: $x \in L \Rightarrow$

$\exists m \quad \Pr_r[A(x,m,r)=acc] \geq 2/3$

Sound: $x \notin L \Rightarrow$

$\forall m: \Pr_r[A(x,m,r)=acc] \leq 1/3$



Amplify

$\exists m, \Pr_r[A(x,m,r)=acc] \geq 1 - \frac{1}{2^{\ell+2}}$

where $m \in \{0,1\}^{\ell}$

$\forall m, \Pr_r[A(x,m,r)=acc] \leq \frac{1}{2^{\ell+1}}$

C: $x \in L \Rightarrow \exists m \quad \Pr_r[A(x,m,r)=acc] \geq 1 - \frac{1}{2^{\ell+2}}$

$\Rightarrow \Pr_r[\exists m, A(x,m,r)=acc] \geq 1 - \frac{1}{2^{\ell+2}}$

S: $x \notin L \Rightarrow \forall m. \Pr_r[A(x,m,r)=acc] \leq \frac{1}{2^{\ell+2}}$

$$\Pr_r[\forall m. A(x,m,r)=acc]$$
$$= 1 - \Pr_r[\exists m, A(x,m,r) \neq acc]$$
$$\leq 1 - \sum_m \Pr_r[A(x,m,r) \neq acc]$$
$$\leq 1 - \sum_m \frac{1}{2^{\ell+1}} \leq 1 - 2^{\ell} \cdot \frac{1}{2^{\ell+2}} = \frac{1}{4}$$

— Hence, $MA \subseteq AM$

Extend the same proof, for any constant k

$$AM[k] \subseteq AM[1] = AM$$

Properties of AM proof systems

(1) $PSPACE \subseteq AM[poly]$ (last lecture)

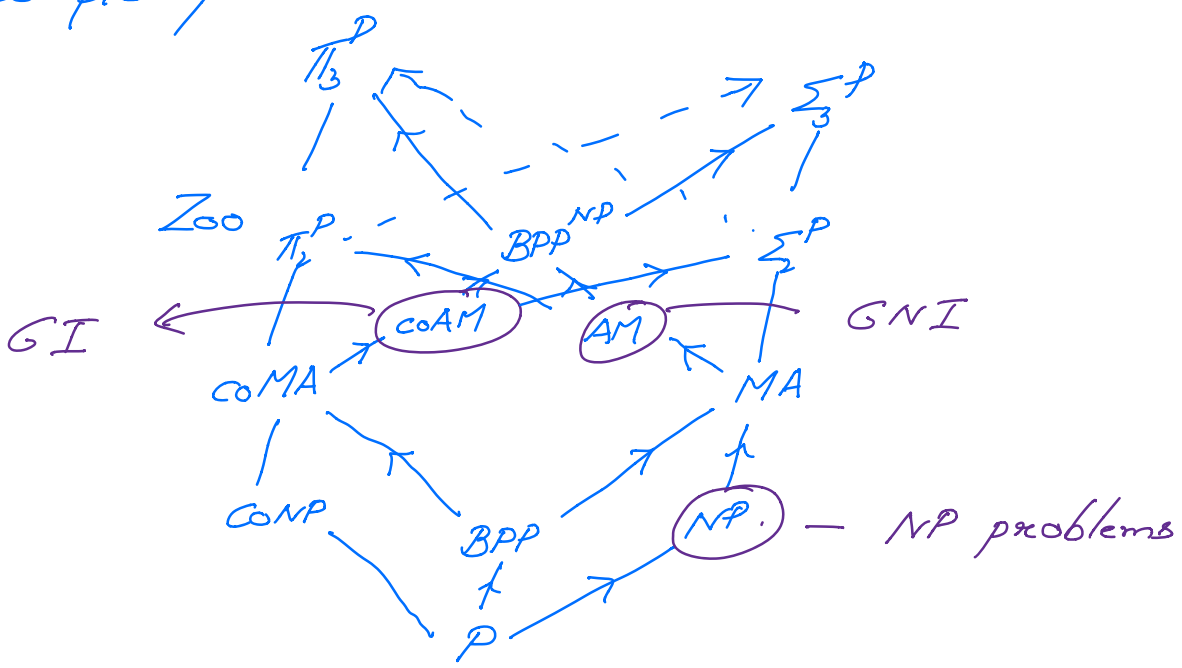
(2) $IP[k(n)] \subseteq AM[k(n)+1]$ (later today)
private coins public

(3) $\forall$ constants k,
$AM[k] \subseteq AM[1] = AM$ (pset 5)

(4) $AM[k(n)]$ - has perfect completeness (pset 6)

Cor. $GNI \in IP[1] \overset{(2)}{\subseteq} AM[2] \overset{(3)}{\subseteq} AM$

Complexity Zoo



Thm: If $NP \subseteq coAM$ (or equivalently $coNP \subseteq AM$) then $PH = AM \subseteq \Pi_2^P$

Pf: $\Sigma_2^P = \exists x \forall y \varphi(x,y)$

$x \to M$; $\forall y \varphi(x,y)$ — coNP statement $\to$ AM

} MAM protocol for Σ_2^P

Any $L \in \Sigma_2^P \Rightarrow L \in MAM \subseteq AM$

$coNP \subseteq AM \Rightarrow \Sigma_2^P \subseteq MAM \subseteq AM \subseteq \Pi_2^P$ (item 3)

If GI is NP-complete

GNI - coNP-complete

$GNI \in IP[1] \subseteq AM[2] \subseteq AM[1] = AM.$

Hence, $coNP \subseteq AM$

PH collapses to AM

Cor: GI is NP-complete, then $PH = \Sigma_2^P$ (Contact to AM)

(3 different proofs of corollary all using IP)

① - above, ② - Arora-Barak ③ - pset 5.

Recently

[Babai] GI has a quasi-poly time algorithm.

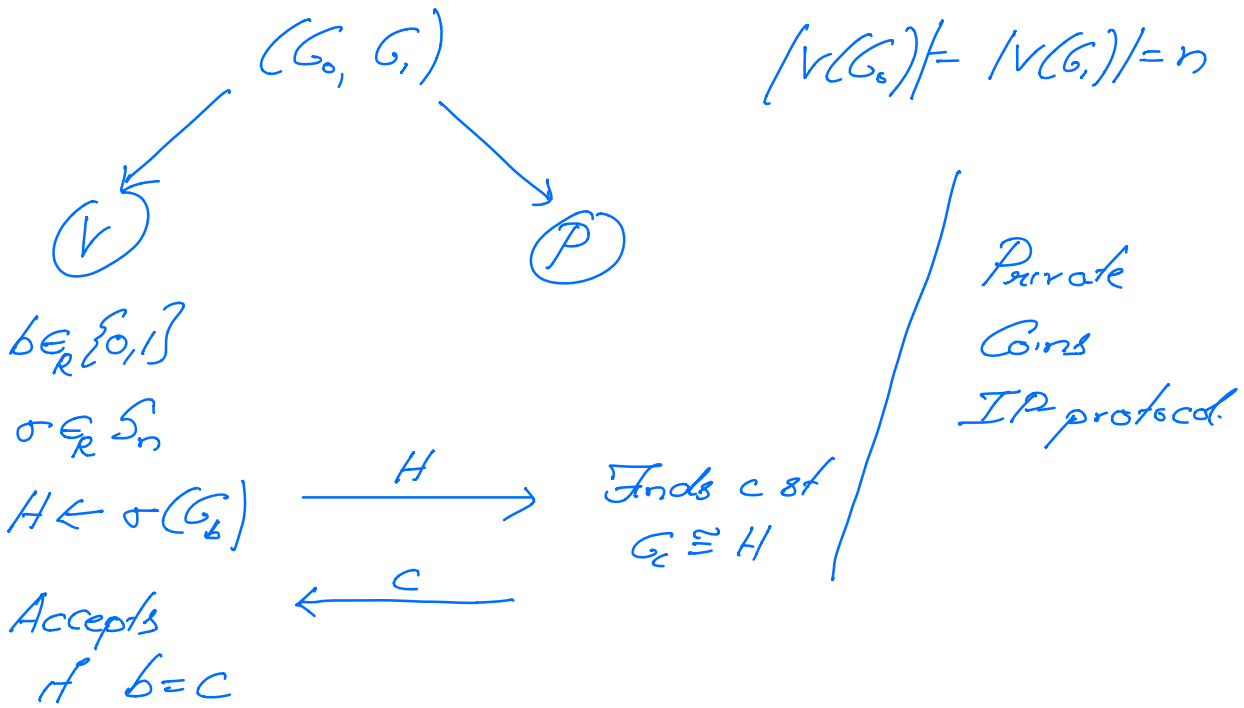
Rest of lecture

Goldwasser-Sipser: Public Coins = Private Coins

Thm [GS] $IP[k] \subseteq AM[k+1]$

Special case: $GNI \in AM[2]$ protocol.

Recall private coins protocol for GNI



$$S = \{H \mid H \cong G_0, \text{ or } H \cong G_1\}$$

- set of messages sent by V to P in first message.

For starters, let us assume both G_0 & G_1 do not have any automorphisms (relabelings of G is identical to relabeled graph)

$G_0 \ncong G_1 \Rightarrow |S| = 2(n!)$

$G_0 \cong G_1 \Rightarrow |S| = n!$

Remove the assumption, redefine

$$S = \{(H,\pi) \mid \exists b \in \{0,1\},\ H \cong G_b \text{ & } \pi \in S_n,\ \pi(H) = H\}$$

$G_0 \not\cong G_1 \Rightarrow |S| = 2(n!)$

$G_0 \cong G_1 \Rightarrow |S| = n!$

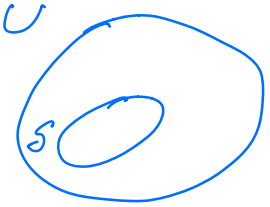
Remarks:

(1) Size of S is different in YES & NO cases
(in particular, large YES
small NO
& a gap between the 2 cases)

(2) Membership in S can be checked w/ a proof

$(H,\pi) \in S \Rightarrow \underbrace{b, \sigma}_{NP\text{-proof}}$ s.t. $\sigma(G_b) = H$
$\pi(H) = H$

U = Graphs on n vertices $\times$ S_n (set of permutations) $\subseteq \{0,1\}^{n^2} \times \{0,1\}^{n \log n}$



YES: $|S| \geq k$
NO: $|S| \leq k/2$.

$k = 2n!$

"$(H,\pi) \in S$" has an NP-proof.

Prover wants to convince via a public coins protocol that S is large.

Set Lower Bound Protocol

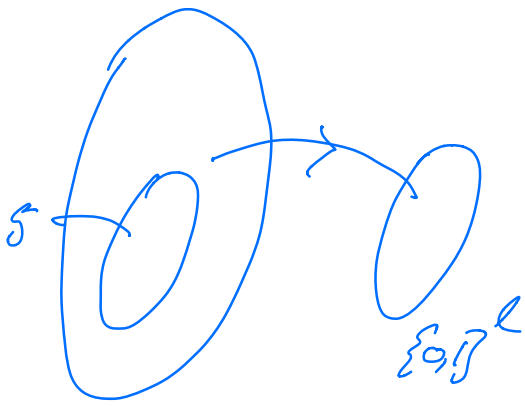
Input: m ; $U = \{0,1\}^m$, $K \in [1, 2^m]$

$S \subseteq \{0,1\}^m$ - specified implicitly via an NP-oracle

Goal: Distinguish. $\begin{cases} |S| \geq K \\ \text{or} \\ |S| \leq K/2. \end{cases}$

Idea: Pairwise independent hash fns.

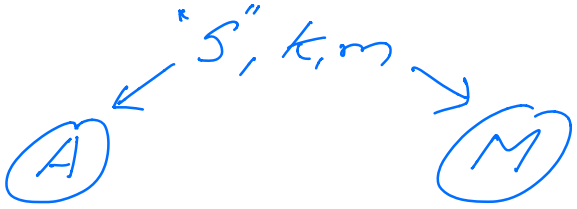
Find ℓ s.t $2^{\ell-2} < K \leq 2^{\ell-1}$



$h : \{0,1\}^m \to \{0,1\}^\ell$

Key Observation: If S is large, most elts in $\{0,1\}^\ell$ have a preimage in S

② If S is small, most elts do not have a pre-image in S.



$\mathcal{H}$ = pairwise ind family of hash fns $\{0,1\}^m \to \{0,1\}^\ell$

$h \in_R \mathcal{H}$, $y \in_R \{0,1\}^\ell$ $\xrightarrow{h, y}$

Verifier acc if $\xleftarrow{s,\ \text{proof}(s \in S)}$

① $h(s) = y$
② proof $(s \in S)$
Accept

Soundness: $|S| \le k/2 \Rightarrow \Pr_{h,y}[\exists s \in S,\ h(s) = y] \le 1/4$

Pf: For every $h : \{0,1\}^m \to \{0,1\}^\ell$

$$\Pr_y[\exists s \in S,\ h(s) = y] \le \sum_{s \in S} \Pr_y[h(s) = y]$$

$$= \sum_{s \in S} \frac{1}{2^\ell} \le \frac{k/2}{2^\ell} \le \frac{k}{2^{k+1}}$$

$=$ ∎

Completeness: $|S| \geq k \Rightarrow \Pr_{h,y}[\exists s, h(s)=y] \geq \ldots$

Pf: $\forall x \; y \in \{0,1\}^\ell$; $\forall x$ $S^* \subseteq S$ s.t. $S^* = k$

$$\Pr_h[\exists s \in S, h(s)=y] \geq \Pr_h[\exists s \in S^*, h(s)=y]$$

$$\geq \sum_{s \in S^*} \Pr_h[h(s)=y] - \sum_{\{s,s'\} \; s \neq s'} \Pr_h[h(s)=h(s')=y]$$

$$= \frac{|S^*|}{2^\ell} - \binom{|S^*|}{2} \frac{1}{2^{2\ell}} \quad \text{(pairwise ind.)}$$

$$\geq \frac{|S^*|}{2^\ell}\left(1 - \frac{|S^*|-1}{2 \cdot 2^\ell}\right) \quad (|S| \geq k \geq 2^{\ell-2})$$

$$\geq \frac{|S^*|}{2^\ell}\left(1 - \frac{|S^*|}{2 \cdot 2^\ell}\right)$$

$$\geq \frac{3}{4} \frac{|S^*|}{2^\ell} \geq \frac{3}{4} \cdot \frac{k}{2^\ell}$$

YES: $\Pr[\text{acc}] \geq \frac{3}{4} \cdot \frac{k}{2^\ell}$

NO: $\Pr[\text{acc}] \leq \frac{1}{2} \cdot \frac{k}{2^\ell}$

$GNI \in IP[1] \subseteq AM[1]$

Next: Zero-knowledge proof systems ∎